No. 19-01204

United States Court of Appeals for the Fourth Circuit

FRANK HEINDEL; PHIL P. LEVANTIS,

Plaintiffs-Appellants,

v.

MARCI ANDINO, Executive Director of the South Carolina State Election Commission, in her official capacity; JOHN WELLS, Chair of the South Carolina State Election Commission, in his official capacity; CLIFFORD J. ELDER, AMANDA LOVEDAY, SCOTT MOSLEY, Members of the South Carolina State Election Commission, in their official capacity,

Defendants-Appellees.

On Appeal fom the United States District Court for the South Carolina, Columbia Division, No. 3:18-cv-01887-JMC

BRIEF OF NATIONAL SECURITY PROFESSIONALS AS *AMICI CURIAE* IN SUPPORT OF NEITHER PARTY

JOSHUA A. GELTZER
MARY B. MCCORD
INSTITUTE FOR CONSTITUTIONAL ADVOCACY AND PROTECTION
600 New Jersey Ave., NW
Washington, DC 20001
Telephone: (202) 661-6728
jg1861@georgetown.edu

KWAKU A. AKOWUAH
CHRISTOPHER C. FONZONE
DAVID MCALOON
GABRIEL SCHONFELD
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
Telephone: (202) 736-8000
Facsimile: (202) 736-8711
kakowuah@sidley.com

Counsel for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 19-01204 Caption: Frank Heindel et al. v. Marci Andino et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Amici National Security Professionals
(name of party/amicus)

who is Amici Curiae, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: /s/ Kwaku A. Akowuah Date: 04/15/2019

Counsel for: Amici Curiae

CERTIFICATE OF SERVICE

****

I certify that on 04/15/2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/ Kwaku A. Akowuah (signature) 04/15/2019 (date)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTEREST OF AMICI CURIAE

Amici Curiae[1] are former national security officials who have substantial experience addressing cyber threats posed by foreign actors. Amici have worked at senior levels in administrations of both political parties and share deep concern about the security of the United States' election systems.

Amici take no position on whether Plaintiffs have standing, and therefore write in support of neither party.[2] They have filed this brief to bring to the Court's attention two key points: (1) that foreign actors have the means and the motive to interfere in U.S. elections, have done so in the past, and will attempt to do so again; and (2) that South Carolina's especially vulnerable election infrastructure makes it a particularly attractive target for foreign adversaries. Amici are concerned that the District Court's reasoning appears to reflect a misunderstanding of these critical points, and offer this brief to ensure proper appreciation of the vulnerabilities and threats associated with election security.

[1] The Amici Curiae certify that no counsel for a party authored this brief in whole or in part; that no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief; and that no person other than the amici or their counsel made a monetary contribution to its preparation or submission. The views expressed herein reflect those of the Amici Curiae but not those of any academic or other institution with which they are affiliated.

[2] All parties consent to the filing of this brief.

LIST OF AMICI CURIAE

Merritt Baer served as Senior Technology Advisor to the Department of Homeland Security and Lead Cyber Advisor to the Federal Communications Commission.

Patrick Barry served as Counselor for Counterterrorism and Intelligence in the Office of the Secretary at the Department of Homeland Security.

Rand Beers served as Acting Secretary of Homeland Security and Undersecretary of the National Protection and Programs Directorate at the Department of Homeland Security.

J. Michael Daniel served as Special Assistant to the President and Cybersecurity Coordinator at the National Security Council staff.

Joshua A. Geltzer served as Senior Director for Counterterrorism and Deputy Legal Advisor at the National Security Council staff and as Counsel to the Assistant Attorney General for National Security.

Dipayan Ghosh served as Senior Advisor on Technology Policy at the Office of Science and Technology Policy and National Economic Council.

Oona A. Hathaway served as Special Counsel to the General Counsel for National Security Law at the Department of Defense.

Robert Knake served as Director for Cybersecurity Policy at the National Security Council staff.

Mary B. McCord served as Acting Assistant Attorney General for National Security and Principal Deputy Assistant Attorney General for National Security.

Matthew G. Olsen served as Director of the National Counterterrorism Center at the Office of the Director of National Intelligence, Deputy Assistant Attorney General for the National Security Division at the Department of Justice, and Special Counsel to the Director of the Federal Bureau of Investigation.

Christopher Painter served as Coordinator for Cyber Issues at the Department of State.

Daniel Rosenthal served as Director for Counterterrorism at the National Security Council staff, Senior Counsel to the Assistant Attorney General for National Security, and Senior Legal Counsel in the Office of the Director of National Intelligence.

Phil Stupak served as Elections Counsel to the House of Representatives, Staff Attorney to the New York City Board of Elections, and Senior Advisor to the Deputy Secretary of the Department of Homeland Security.

Francis Taylor served as Undersecretary of the Office of Intelligence and Analysis at the Department of Homeland Security.

James C. Trainor served as Assistant Director for the Cyber Division at the Federal Bureau of Investigation.

INTRODUCTION

Foreign interference in U.S. elections is a persistent and intensifying national security challenge. Unable to match our Nation's military might or diplomatic reach, foreign actors have long sought to manipulate and undermine our elections, and the emergence of modern communications technologies has made it easier for them to do so. The risk is real, and it is growing. Moreover, the state of our election infrastructure only magnifies these risks. Direct tampering with the vote-counting process by foreign actors would strike directly at the heart of our democracy, and would likely diminish public confidence in it. Yet the tools used in parts of the United States to store voter rolls and to collect and tabulate votes remain deeply vulnerable to attack and a prime target for foreign adversaries. Outdated systems like South Carolina's iVotronic voting machines are among the most vulnerable.

Amici take no position on whether Plaintiffs have standing, but write because the District Court's analysis does not appear to reflect a full appreciation of these vulnerabilities and threats. The District Court indicated that the passage of time since Russia's well-documented interference in the 2016 presidential election rendered speculative the risk of future election interference. D. Ct. Op. at 20. The District Court also questioned whether the acknowledged flaws in South Carolina's voting machines would make them a prime target for foreign attackers. D. Ct. Op. at 20-23.

Based on their experience in addressing election interference and knowledge of national security matters, Amici believe that both of those suggestions by the District Court are mistaken. First, as the Director of National Intelligence has frequently warned, the threat of foreign vote tampering is substantial. Foreign actors have abundant reason to seek to interfere with U.S. elections, and history shows that they have attempted to do so repeatedly. There is every reason to believe they will attempt to do so again in the future. The events of 2016 were thus not a one-time threat, but rather a warning sign about how foreign actors likely will attempt to manipulate our elections in the digital age.

Second, Amici dispute the notion that South Carolina's voting machines are not a comparatively attractive target. To be sure, foreign actors do not solely focus on ease of access when deciding which parts of the U.S. election infrastructure to attempt to infiltrate. But adversaries are of course more likely to engage in operations they think will be successful, and they accordingly are more likely to target infrastructure that can be easily overcome. South Carolina iVotronic voting machines not only have numerous publicly documented security flaws, but also lack the basic auditability that would help identify or remediate an attack. They are thus a particularly attractive target.

I. Foreign Actors Have the Means and the Motive to Interfere in U.S. Elections, Have Done So in the Past, and Will Attempt to Do So Again.

It is well documented that the United States faces an ongoing threat of foreign election interference. Nevertheless, the District Court suggested that the risk of foreign tampering could not go on "for an indefinite amount of time," and would become more uncertain as Russia's 2016 interference recedes into the past. D. Ct. Op. at 20. The experience and judgment of national security experts counsel against this understanding of the threat now facing our elections.

Free and fair elections are fundamental to our political system. Elections channel the popular will into government action, and do so in a way that gives the electorate confidence that the Government is deriving its power "from the great body of the people." James Madison, Federalist No. 39. As the Supreme Court has put it, the "right to vote freely for the candidate of one's choice is of the essence of a democratic society." *Reynolds v. Sims*, 377 U.S. 533, 555 (1964).

This centrality of elections to the U.S. system of government is precisely what makes them a particularly attractive target for foreign actors. Because the United States makes choices about how it will govern itself through popular voting, foreign actors know that the election of candidates expected to pursue their favored policies will help to advance their agenda. *See* Office of the Director of National Intelligence, *Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections*, ICA 2017-01D, at 1 (2017) ("ODNI Report").

Moreover, foreign actors know that even an intervention that does not produce a specific desired electoral outcome can advance their agenda by unsettling our election-based system of governance. Public awareness of foreign interference efforts can both sow discord in the U.S. electorate and "undermine public faith in the U.S. democratic process." *Id.* Indeed, as a recent study concluded, "[v]oters who learned of a foreign intervention—particularly those who learned of active interventions such as . . . hacking voting machines—were substantially more likely to distrust the results of the election, protest the electoral outcome, lose faith in American democracy, and avoid voting in future elections." Michael Tomz and Jessica L.P. Weeks, *Public Opinion and Foreign Electoral Intervention*, presented to 2018 Annual Meeting of the American Political Science Association, Boston, MA (Aug. 2018), *available at* https://web.stanford.edu/~tomz/working/TomzWeeks-ElectoralIntervention-2018-08-24.pdf.

In short, election interference can have significant consequences for American democracy—which is precisely why foreign actors have long have sought to engage in it. *See, e.g.*, Alden Fletcher, *Foreign Election Interference in the Founding Era*, Lawfare (Oct. 25, 2018, 9:09 AM), https://www.lawfareblog.com/foreign-election-interference-founding-era (describing French intervention in support of Thomas Jefferson during the 1796 presidential election); Ladislas Fargo, *The Game of the Foxes: The Untold Story of German Espionage in the United States and Great*

Britain during World War II 387 (David McKay Publications 1972) (noting how, in 1940, Nazi Germany bribed a U.S. newspaper to publish a document it hoped would convince Americans that President Franklin D. Roosevelt was a "warmonger"); Bob Woodward and Brian Duffy, *Chinese Embassy Role in Contributions Probed*, The Washington Post, Feb. 13, 1997 (noting how, during the 1996 presidential campaign, China attempted to direct financial contributions to the Democratic National Committee). During the Cold War, for example, the Soviet Union used influence agents, forged compromising materials, and manipulated American media to harm candidates that it viewed as hostile to its interests. ODNI Report at 5; *see also* Michael Chertoff and Anders Fogh Rasmussen, *The Unhackable Election: What It Takes to Defend Democracy*, Foreign Affairs (Jan./Feb. 2019) (describing Soviet misinformation campaigns during the Cold War). Viewed through this lens, Russia's well-known and multi-faceted campaign to influence the 2016 election is just the latest manifestation of a threat that has long persisted.

Russia's 2016 attacks also show how technological advances have exacerbated the risk of foreign election interference. As the Intelligence Community and intelligence committees in both the Senate and House of Representatives found, Russia's cyberattacks on election infrastructure and social media misinformation campaign "highlighted technical vulnerabilities in U.S. digital infrastructure" and achieved their "primary goal of inciting division and discord among Americans."

House Permanent Select Committee on Intelligence, *Report on Russian Active Measures*, H. Rep. 115-1110, at 1 (2018) ("HPSCI Report")[3]; Senate Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations* 2, 4 (2018) ("SSCI Report") [4]; ODNI Report at ii-iii.

Of particular note here is the finding that Russian-backed actors "conducted an unprecedented, coordinated cyber campaign against state election infrastructure." SSCI Report at 1. Indeed, intelligence reporting suggests that this campaign targeted all 50 states. As a recent Federal Bureau of Investigation and Department of Homeland Security Joint Intelligence Briefing put it:

> Russian cyber actors in the summer of 2016 conducted online research and reconnaissance to identify vulnerable databases, usernames, and passwords in . . . greater than 40 [states]. Despite gaps in our data where some states appear to be untouched by Russian activities, we have moderate confidence that Russian actors likely conducted at least reconnaissance against all US states based on the methodical nature of their research.[5]

---

[3] Available online at https://www.congress.gov/115/crpt/hrpt1110/CRPT-115hrpt1110.pdf.

[4] Available online at https://www.intelligence.senate.gov/sites/default/files/publications/RussRptInstlmt1.pdf.

[5] Sean Gallagher, *DHS, FBI say election systems in all 50 states were targeted in 2016*, Ars Technica (Apr. 10, 2019, 2:20 PM), https://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016/.

The degree of access Russia obtained was notable for not only its breadth, but also its depth. As part of the 2016 campaign, Russian-backed hackers successfully penetrated voter registration databases in multiple states. HPSCI Report at 42. In some instances, these hostile foreign actors compromised those systems so deeply that they were "in a position to, at a minimum, alter or delete voter registration data." SSCI Report at 1-2. In short, although there is no evidence of which Amici are aware indicating that Russia actually did tamper with the vote count in 2016, there is evidence that Russia had the capacity to alter the vote count if it had chosen to do so.

The threat, moreover, continues to grow. Earlier this year, Director of National Intelligence Dan Coats disclosed that unidentified actors targeted United States election infrastructure in 2018, and the best assessment of U.S. intelligence and law enforcement agencies is that more attacks are coming in 2020 and beyond. Director of National Intelligence Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community* 7 (2019) ("DNI Threat Assessment").[6]

As the 2019 DNI Threat Assessment—the Intelligence Community's annual assessment of threats to U.S. national security—puts it, "[o]ur adversaries and strategic competitors probably already are looking to the 2020 U.S. elections as an

[6] Available online at https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

opportunity to advance their interests," and will continue to "refine their capabilities and add new tactics as they learn from each other's experiences." *Id.* at 7.

Importantly, the Intelligence Community also has made clear that the threat is not confined to Russia. *Id.* at 5-7 (flagging cyber capabilities of China, Iran, and North Korea); *see also* Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference* 5, Brennan Center for Justice (2017) ("Brennan Center Report"). A few months prior to the 2018 midterm elections, for example, National Security Advisor John Bolton revealed that there was sufficient "national security concern" about election interference by China, Iran, and North Korea that the federal government was "taking steps to try and prevent it." Carol Morello, *Bolton says four foreign adversaries may try to interfere in U.S. midterms*, The Washington Post, Aug. 19, 2018.[7] Nor is the threat of election interference emerging solely from state actors. Terrorist organizations such as al Qaeda and ISIS have conducted cyberattacks on foreign governments, Brennan Center Report at 5, and could turn their efforts toward elections in the future.

In sum, at almost exactly the same time the district court was suggesting that the risk exemplified by Russia's 2016 election interference efforts was fading into

[7] Available online at https://www.washingtonpost.com/world/national-security/bolton-says-four-foreign-adversaries-may-try-to-interfere-in-us-midterms/2018/08/19/9d8987f8-a3b6-11e8-97ce-cc9042272f07_story.html?utm_term=.0db08156ac0d.

the past, the Intelligence Community was warning precisely the opposite: that future interference efforts may go even further. Hostile actors may not content themselves with canvassing voter rolls and state systems and instead might actually "seek to use cyber means to directly manipulate or disrupt election systems—such as by tampering with voter registration or disrupting the vote tallying process." DNI Threat Assessment at 7; *see also* Secretary of Homeland Security Kirstjen M. Nielsen, *Rethinking Homeland Security in an Age of Disruption*, Address at George Washington University (Sept. 5, 2018) ("Nielsen Remarks") (noting the risk and commenting that the Department of Homeland Security has made election security one of its "highest and continuous priorities," and is working with state and local governments to help secure their network infrastructure).[8]

In other words, the threat is real—and it is not going away. National security professionals in and out of government—Amici Curiae included—take that continuing threat extremely seriously.

II. South Carolina's Particularly Vulnerable Election Infrastructure Is Especially Susceptible to Attack and Therefore a Serious National Security Risk.

A hostile actor's attack on balloting infrastructure would be a particularly damaging form of election interference because it could directly affect the vote count

[8] Available online at https://www.dhs.gov/news/2018/09/05/secretary-nielsen-remarks-rethinking-homeland-security-age-disruption.

and call the integrity of the election into question. And because hostile actors will choose targets based in part on the relative strength or weakness of those targets' defenses, they will likely view South Carolina's vulnerable infrastructure as an especially inviting target. In the understanding and experience of Amici, the District Court erred in downplaying the connection between a state election system's vulnerable defenses and the likelihood of attack by a foreign actor. D. Ct. Op. at 20-24.

A. Attacks on our election infrastructure raise particularly acute national security concens because they strike at the heart of our democracy by directly threatening the vote count and calling into question the integrity of our elections.

Election interference takes many forms, from disinformation campaigns to direct attacks on systems used to register voters, cast ballots, and count votes. As national security officials repeatedly have recognized, however, an attack on either the voter rolls or balloting itself would be potentially devastating. Preventing foreign actors from directly tampering with voting infrastructure is thus a national security priority.

The reasons for this are myriad and flow from the centrality of elections to American democracy itself. For most Americans, "voting machines *are* elections," and direct vote tampering is a "concrete, easy-to-understand method for tampering with elections," Brennan Center Report at 7. While the precise effects of other forms of interference can be difficult to measure, nothing could be clearer in its dramatic

consequences than changing a vote from one candidate to another. And nothing would so quickly diminish the public's confidence in an election's outcome than if it knew that a foreign actor had tampered with particular votes.

Interference with the computerized voter registration databases that states must maintain under the Help American Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (codified at 52 U.S.C. § 21083), presents a similar risk. While such systems play no role in the actual counting of votes, they tell officials *who* may vote. An attack on such a database could disrupt and seriously undermine the legitimacy of an election by interfering with qualified voters' ability to cast a ballot. Brennan Center Report at 14.

For this reason, intelligence and law enforcement agencies, elected officials, and security professionals believe that hardening our entire election infrastructure is a national security imperative. In January 2017, Secretary of Homeland Security Jeh Johnson exercised his authority under the PATRIOT Act to designate the nation's election systems as "critical infrastructure," so that it would be a "priority for [federal] cybersecurity assistance and protections." Department of Homeland Security, *Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector* (Jan. 6, 2017).[9] More recently,

[9] Available online at https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

Secretary Nielsen called on *all* states to ensure that they have redundant, auditable election systems in place for the 2020 elections. *See* Nielsen Remarks.

The House and Senate Select Committees on Intelligence investigating Russia's interference in the 2016 election also advised that the United States' election infrastructure must be fortified for the future, *see* HPSCI Report at 133; SSCI Report at 5-6, a sentiment echoed by a bipartisan group of congressional leaders, *see, e.g.*, Press Release of Senators Lankford, Klobuchar, Harris, Collins, Heinrich and Graham to Introduce Election Security Bill (Dec. 21, 2017). Intelligence and security experts further echo these sentiments and emphasize the need for action.

To this end, recent comments from Former Director of Central Intelligence R. James Woolsey, Jr., are instructive. Unlike Pearl Harbor and the 9/11 attacks, Woolsey has said, the targets of recent cyber attacks were not "ships or airplanes or buildings, but the machinery of our democracy. We will be attacked again. We must act again—or leave our democracy at risk." Brennan Center Report at 2; *see also* Christina Pazzanese, *The worries over U.S. intelligence*, The Harvard Gazette, June 22, 2018 (former Director of National Intelligence James Clapper stressing the need for increased focus on election interference).[10]

[10] Available online at https://news.harvard.edu/gazette/story/2018/06/clapper-frets-over-past-damage-present-shortcomings-future-threats-to-us-intelligence/.

B. South Carolina's insecure voting machines are especially vulnerable and thus a prime target for foreign actors.

There are a wide range of reasons a foreign attacker might choose to attack the election infrastructure of one jurisdiction over another. An attacker may seek to support a favored candidate, or be encouraged to intervene by the prospect of flipping the result in a close contest. Whatever other motives drive attacker considerations, however, a key consideration with respect to every attack will be the likelihood of success. *See* Dov H. Levin, *When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results*, 60 Int'l Studies Q. 189, 190 (2016) (noting that "electoral interventions usually occur when" a would-be attacker has both motive and opportunity); Nat'l Academies of Sciences, *Securing the Vote: Protecting American Democracy* 89 (Nat'l Academies Press 2018) ("NAS Report") (making the point that "stronger defenses increase the time and effort required to conduct an attack," such that "well-defended targets are less attractive" to attackers).

Viewed in this light, South Carolina's iVotronic voting system is particularly vulnerable to attack. Multiple studies have evaluated the security of the system, and found it deeply wanting. *See* Ohio Secretary of State, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing* (2007) ("EVEREST Report"); David A. Eckhardt & Kami Vaniea, PA Verified Voting & VoteAllegheny, *Report on Allegheny Cty. iVotronic Firmware Verification* (Rev. 1.3

2009); Alec Yasinsac et al., Security and Assurance in Information Technology Laboratory, Florida State University, *Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware* (2007); Douglas W. Jones, Department of Computer Science, University of Iowa, *Recommendations for the Conduct of Elections in Miami-Dade County Using the ES&S iVotronic System* (2004). Indeed, as laid out below, it is likely that South Carolina's system is one of the most vulnerable in the country and thus a distinctively attractive target.

We do not have the space to repeat every aspect of the analysis found in the studies of the iVotronic system or to detail every security flaw that those studies uncovered. Rather, we instead focus on identifying a few key points that epitomize the systems' vulnerabilities.

To begin, the basic design of South Carolina's election system means that it provides no audit trail or other way reliably to discover election interference. It is axiomatic that in computing "[t]here is no such thing as perfect security," Niels Ferguson, Bruce Schneier & Tadayoshi Kohno, *Cryptography Engineering: Design Principles & Practical Applications* 10 (Wiley Publ'g, Inc. 2010), and that "computer [voting] systems, [therefore], no matter how well constructed, cannot anticipate and prevent all the possible means of attack." NAS Report at 89. Thus, because electronic balloting can never be fully secure from cyber threats, a reliable audit trail is necessary for confidence in any voting system with an electronic

component. In short, jurisdictions "must adopt methods that can assure the accuracy of the election outcome without relying on the [integrity of] hardware and software used to conduct the election." *Id.* at 91.

But South Carolina's voting machines—known as "paperless direct recording electronic" or "paperless DRE" voting machines—cannot do this. Paperless DRE machines record votes in digital memory only and do not create a paper trail. Danielle Root et al., Center for American Progress, *Election Security in All 50 States* 6 (2018). Thus, by design, paperless DRE machines lack any record of a voter's intention that is independent from the electronic system itself. To be audited, however, a voting system must produce a voter-verified, human-readable paper trail so that election officials can count each ballot without any risk that a compromised computer is lying to them. NAS Report at 82 n.83 (citing Ronald L. Rivest, *On the Notion of "Software Independence" in Voting Systems*, Philosophical Transactions of the Royal Society A, 10.1098/rsta.2008.0149 (Oct. 28, 2008)). South Carolina's system of paperless DRE voting makes such assurances impossible.[11]

[11] The iVotronic system also may create a false sense of security in election officials by producing "audit logs" that cannot actually be used to conduct a meaningful audit. Each voting machine in South Carolina stores two copies of each vote: one in built-in memory that is transferred to the central tabulating computer at the end of election days, and one on a removable memory card that is saved for "audit" purposes. EVEREST Report at 35. In theory, election officials could attempt to detect irregularities by comparing the tabulated data to the "audit" data. But, because both sets of data are produced by the voting machine itself, that comparison could not reliably detect if a machine had been compromised. An

Moreover, the risks posed by the iVotronic system's lack of auditability are compounded by the insecurity of South Carolina's voting system. As a leading security researcher recently stated at a congressional hearing on elections, security is "especially imperative" where the "accuracy and integrity of the recorded vote tally depends *completely* on the correctness and security of the [voting] machine's hardware, software, and data." *Hearing on Cybersecurity of Voting Machines Before the Subcomms. on Info. Tech. and Intergovernmental Affairs of the H. Comm. on Oversight and Gov't Reform*, No. 115-64, at 37 (2017) ("Joint Hearing") (Statement of Matt Blaze, Professor, University of Pennsylvania) (emphasis added). South Carolina's use of paperless DRE machines ensure that this dependency exists here, but its voting system does not have in place the protection necessary to cover for its lack of auditability.

Consider the "several pervasive, critical failures" identified by security researchers:

- The voting machines themselves "can be easily tampered with in the field." EVEREST Report at 29.

attacker could easily change any altered votes in *both* records, and auditors would be unable to do anything more than compare the corrupted system against itself.

- The machines' basic software can be compromised through interfaces that are exposed to ordinary voters, "without knowledge of passwords and without the use of any specialized proprietary hardware." *Id.*
- Moreover, the iVotronic system's central tabulating and election management software, although not exposed to voters directly, "is vulnerable to attacks that exploit coding and design errors and that can be triggered from data sent from the field." *Id.*

These are not hypothetical attacks only possible under laboratory conditions. They are "practical threats" to South Carolina's elections, and researchers were unable to "identify [any] practical procedural safeguards that might substantially increase the security of the . . . system in practice." *Id.* at 30.

Nor should election officials take any comfort from the fact that the researchers who identified these vulnerabilities had access to the iVotronic system's source code and documentation. Experience has shown that "technical minds with little or no previous knowledge about voting machines, [even] without . . . documentation or tools, can still learn how to hack the machines within tens of minutes or a few hours." Matt Blaze et al., *DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases,*

and Infrastructure 14 (2017).[12] When hackers were given access to six paperless DRE machines—including the iVotronic—for only three days, "every piece of equipment . . . was effectively breached in some manner." *Id.* at 4, 16.

One potential attack identified by security researchers, which would exploit several vulnerabilities in combination to take over a county's entire election infrastructure, is particularly illustrative of the vulnerability of South Carolina's system. Every South Carolina voting machine has a front-facing slot, designed to accept a "Personalized Electronic Ballot," or PEB. Each PEB is a small handheld computer, EVEREST Report at 33, 37, and inserting a PEB into a voting machine will prompt the machine to take different actions depending on the PEB's programming, *id.* at 50. The PEB and voting machine communicate through infrared light signals—essentially the same technology used in television remote controls. *Id.*

The software that governs the interactions between the PEB and the voting machine, however, has a serious vulnerability. It allows any attacker able to gain physical access to a PEB slot—access afforded every South Carolina voter—to "load malicious software that takes complete control over the [terminal's] processor." EVEREST Report at 55. The consequences could be substantial. Because it permits

[12] Available online at https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

"complete control" of a voting terminal, an attacker could "alter the terminal firmware, change recorded votes, mis-record future votes, and so on throughout the election day and in future elections." *Id.*

Carrying out this attack would not need to be complex. All that an attacker needs in order to exploit this vulnerability is physical access to a voting terminal's PEB slot, and a device loaded with malicious code that the terminal will treat as a PEB. The PEB slot is located on the front of each voting terminal, only an inch or so away from the voting touchscreen, and "it is difficult for poll workers to monitor for [suspicious behavior] . . . without sacrificing voter privacy." EVEREST Report at 65. Moreover, researchers have determined that any handheld computer (the researchers used a Palm Pilot) capable of transmitting data over infrared, in combination with a handheld magnet strong enough to trip the voting terminal's magnetic switch, can easily present itself to a voting terminal as a legitimate PEB. *Id.*

The risk is not limited to individual voting machines. Security researchers have found that the iVotronic system's central tabulation and election management software is also vulnerable. EVEREST Report at 59. That vulnerability "can be exploited when election . . . results are processed" from a PEB purporting to contain vote tallies downloaded from voting machines. *Id.* Because the malicious code can be hidden in vote tallies, and PEBs with vote tallies must be brought to election

headquarters in order to count votes, an attacker would not need either physical or internet access to the central server in order to carry out this attack. EVEREST Report at 53. The attacker would need only to compromise a single PEB from a single precinct. That would allow an attacker "to gain full control of the machine running the [central election management] server," and to "install[] a virus or Trojan that could then be used to change the election results and spread the virus to other" components of the voting system. *Id.* at 59-60.

In other words, these flaws allow every component of South Carolina's voting system to exploit every other component, including the central election management system. Thus, "[i]nserting malicious code at any step in this process could result in a virus spreading to all of the other components, completely compromising the election." *Id.* at 98. Indeed, an attacker able to compromise even a single PEB in a single precinct could introduce a "persistent viral infection of malicious code in . . . [a county's entire] electronic voting infrastructure," using nothing more than a magnet and a Palm Pilot. *Id.*

Even relative to other American jurisdictions, then, South Carolina's voting system is notably insecure. South Carolina is one of only five states—along with Delaware, Louisiana, Georgia, and New Jersey—that, despite the widely publicized vulnerability of paperless DRE machines, continues to use such systems exclusively. Blue Ribbon Commission on Pennsylvania's Election Security, *Study and*

Recommendations 20 (2019) ("Pennsylvania Report"). Delaware and Louisiana, however, are in the process of phasing those machines out of use. *Id.* Moreover, the number of states that use paperless DRE machines *at all* has been shrinking and will likely continue to do so: Virginia phased out its paperless DRE machines in favor of paper ballots in time for its 2017 elections. Joint Hearing at 21 (Statement of Edgardo Cortes, Commissioner, Virginia Department of Elections). Pennsylvania has also made the decision to switch to all-paper voting. Pennsylvania Report at 22. Considering the attention brought to election interference in 2016, and the emergence of a "consensus view" among security experts in favor of paper balloting, *id.*, this trend is likely to continue. And as South Carolina clings to its inadequate system and the number of other states using this insecure technology shrinks, South Carolina's elections may stand out as an especially vulnerable target for foreign adversaries seeking to interfere in our elections.

CONCLUSION

Foreign actors have interfered in our elections before, are likely to do so again, and have enough common sense to aim at easy targets. The District Court discounted each of these alarming facts, which the national security community accepts across party lines. Amici take no position on the ultimate question of whether Plaintiffs have standing, but urge this Court to decide the case on a basis that aligns with the troubling but powerful evidence that there is now a present and grave threat that

foreign hackers will target South Carolina's voting system in the 2020 election cycle and beyond.

Dated: April 15, 2019

Respectfully submitted,

/s/ Kwaku A. Akowuah

Kwaku A. Akowuah
Christopher C. Fonzone
David McAloon
Gabriel Schonfeld
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: (202) 736 8000
Facsimile: (202) 736 8711
kakowuah@sidley.com

Joshua A. Geltzer
Mary B. McCord
INSTITUTE FOR CONSTITUTIONAL ADVOCACY AND PROTECTION
600 New Jersey Avenue, NW
Washington, DC 20001
Telephone: (202) 661-6728
jg1861@georgetown.edu

Attorneys for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
Effective 12/01/2016

No. 19-01204 **Caption:** Frank Heindel et al. v. Marci Andino et al.

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMIT

Type-Volume Limit, Typeface Requirements, and Type-Style Requirements

Type-Volume Limit for Briefs: Appellant's Opening Brief, Appellee's Response Brief, and Appellant's Response/Reply Brief may not exceed 13,000 words or 1,300 lines. Appellee's Opening/Response Brief may not exceed 15,300 words or 1,500 lines. A Reply or Amicus Brief may not exceed 6,500 words or 650 lines. Amicus Brief in support of an Opening/Response Brief may not exceed 7,650 words. Amicus Brief filed during consideration of petition for rehearing may not exceed 2,600 words. Counsel may rely on the word or line count of the word processing program used to prepare the document. The word-processing program must be set to include headings, footnotes, and quotes in the count. Line count is used only with monospaced type. See Fed. R. App. P. 28.1(e), 29(a)(5), 32(a)(7)(B) & 32(f).

Type-Volume Limit for Other Documents if Produced Using a Computer: Petition for permission to appeal and a motion or response thereto may not exceed 5,200 words. Reply to a motion may not exceed 2,600 words. Petition for writ of mandamus or prohibition or other extraordinary writ may not exceed 7,800 words. Petition for rehearing or rehearing en banc may not exceed 3,900 words. Fed. R. App. P. 5(c)(1), 21(d), 27(d)(2), 35(b)(2) & 40(b)(1).

Typeface and Type Style Requirements: A proportionally spaced typeface (such as Times New Roman) must include serifs and must be 14-point or larger. A monospaced typeface (such as Courier New) must be 12-point or larger (at least 10½ characters per inch). Fed. R. App. P. 32(a)(5), 32(a)(6).

This brief or other document complies with type-volume limits because, excluding the parts of the document exempted by Fed. R. App. R. 32(f) (cover page, disclosure statement, table of contents, table of citations, statement regarding oral argument, signature block, certificates of counsel, addendum, attachments):

☑ this brief or other document contains 5,365 [*state number of*] words

☐ this brief uses monospaced type and contains _____ [*state number of*] lines

This brief or other document complies with the typeface and type style requirements because:

☐ this brief or other document has been prepared in a proportionally spaced typeface using
_____ [*identify word processing program*] in
_____ [*identify font size and type style*]; **or**

☐ this brief or other document has been prepared in a monospaced typeface using
_____ [*identify word processing program*] in
_____ [*identify font size and type style*].

(s) Kwaku A. Akowuah

Party Name Amici Curiae

Dated: 04/15/2019

CERTIFICATE OF SERVICE

I certify that on April 15, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/ Kwaku A. Akowuah
Signature

04/15/2019
Date